



The state of legal and regulatory risk management: Questions for corporate directors

By Josée Morin, Eng., MBA, C.Dir., jo.morin@videotron.ca

The following is a generic list of questions that to help corporate directors evaluate the state of regulatory and legal risk management in a business that is starting to implement a structured risk management approach. There may be risks that are not covered in this list or questions that do not apply to your situation.

Legal and regulatory compliance

1. What are the main legal and regulatory requirements that we must respect to conduct business?
2. How are we keeping an eye on new laws and regulations and how they may affect us?
3. What are the employees that need to be and are aware of legal and regulatory requirements? Do we do training on this subject to keep them up to date?
4. How do we ensure compliance with these laws and regulations? Are we doing compliance audits? How often and what do they cover? What are the usual outcomes?
5. How are non-conformities identified and tracked? How often do they occur?
6. What would be the impact if we did not detect non-compliance or did not comply with a law or regulation, on dollars or other terms?
7. When looking at mergers and acquisitions, are we paying special attention to the legal and regulatory risks of our partners and to nonconformities? If so who is responsible for that?
8. How do we ensure compliance with the terms and conditions of contracts with our suppliers and customers, including software licenses?

Ethics and fraud

9. Is there a code of ethics signed by employees and is it well known and followed? How often is ethics training being done?

10. Are there policies and procedures for detecting internal and external fraud? Has there been any fraud? Can employees report fraud anonymously?

11. Is there any potential for fraud from our business relationships?

Quality assurance of products developed internally

12. How is quality assurance managed for products we develop? Do we have clear and documented standards and specifications that must be met? Is the testing process documented, etc.?

13. Are there performance guarantees we provide to our customers? Do these guarantees put us at risk? What is our history?

14. Is product labeling complex and error prone?

Protection of sensitive information and knowledge

15. How do we store, identify and protect sensitive documents for the conduct of our business, for example intellectual property, contracts, etc.? Is there a policy on that topic?

16. Has the organization developed and implemented formal information security and privacy policies?

17. Do we ensure that the policies are followed? How?

18. Are there any restrictions on who may have access to personal information, do we keep data access registries, etc.?

19. How are intangible assets protected, such as copyrights, trademarks, and commercial secrets?

Health and Safety

20. Are there procedures in place for occupational health and safety? What are our main risks in these areas?